RINGS WITH A FINITE NUMBER OF PRIMES. I

BY
I. S. COHEN AND IRVING KAPLANSKY

1. **Introduction.** Suppose R is an integral domain having a finite number of non-associated primes $p_1, \cdots, p_n$, and suppose further that any element of R can be expressed as a product of primes. We are interested in the possible structure of R, and in particular in its multiplicative structure. If factorization is unique, then (modulo units) we simply have the free multiplicative semigroup with generators $p_1, \cdots, p_n$. If factorization is not unique, there are relations among the p's. However the fact that R must submit to addition as well as multiplication serves to eliminate most of the relations which are a priori possible. For example, $n=2$ is impossible, and for $n=3$ we must have (modulo units) $p_1p_2=p_3^2$, and cyclically.

The present paper originated in an attempt to obtain analogous results for larger values of n. After a preliminary reduction to the case of a local ring, we are able to settle completely the case where n is prime: the multiplicative structure is unique and generalizes the result cited above for $n=3$. Moreover we obtain a number-theoretic criterion which is necessary and sufficient for the existence of such rings.

The investigation of the more difficult case of composite n is still in progress. The results will be presented in a subsequent paper.

2. **Reduction to a local ring.** The letter R will always denote an integral domain with unity element satisfying the conditions:

(a) Every element of R can be expressed as a product of prime elements.

(b) There are but a finite number of prime elements in R.

By a *prime element* of R is meant a non-unit which cannot be factored into non-units. A non-unit p is certainly prime if its principal ideal (p) is prime; but this condition is not necessary. Indeed, if (p) is a prime ideal for every prime element p, then factorization is unique.

Condition (a) is satisfied if R is Noetherian—that is, if the ascending chain condition holds for the ideals of R; but this chain condition is not necessary, as is shown by the example of a polynomial ring in infinitely many variables.

Condition (b) means of course that the number of non-associated primes is finite. An example of a ring satisfying this condition (as well as (a)) is the set of all rationals which can be written with denominator not divisible by any of a given finite set of prime integers. This ring, however, is trivial in the sense that factorization is unique and there is nothing to study in the multiplicative structure. Nontrivial examples will be given later.

Presented to the Society, September 15, 1945; received by the editors April 10, 1946.

It is perhaps of interest to see first what can be accomplished by very simple arguments. Suppose that factorization in R is not unique; then there exists a prime p such that (p) is not a prime ideal. If P is any prime ideal[1] containing (p), then P must contain a second prime q. Now $p+q$ is in P and is therefore a non-unit. However $p+q$ is divisible by neither p nor q; hence P must contain a third prime r. We have thus shown that non-unique factorization requires the presence of at least three primes in R. Suppose R has exactly three primes, p, q, r, all necessarily in one prime ideal. Then $qr+p$ is a non-unit and is not divisible by q or r; it must be divisible by p. Hence so is qr, and we have $qr=\alpha p^a$ where α is a unit and a an integer not less than 2. Similarly $rp=\beta q^b$, $pq=\gamma r^c$. Multiplying and cancelling, we obtain $a=b=c=2$. This uniquely defines the multiplicative structure of R modulo units. That this ring can actually arise is shown later (Theorem 13).

The treatment of rings with four or more primes requires a deeper discussion which we initiate with the following theorem.

THEOREM 1. *Two maximal ideals of R cannot have a prime element in common.*

Proof. A maximal ideal is prime and therefore has a basis of prime elements. It follows that there are only a finite number of maximal ideals: say $M_1, \cdots, M_h$. Suppose the prime r is in $M_1 \cap M_2$. Since M_1 is not contained in any of $M_2, \cdots, M_h$, it contains an element—and hence also a prime element—not in any of these. Let $p_1, \cdots, p_k$ $(k>0)$ be those primes not in any of $M_2, \cdots, M_h$, hence in M_1. Let a_i $(2 \leqq i \leqq h)$ be in M_i but not in M_1, and set $a=a_2 \cdots a_h$. Then a is in $M_2 \cap \cdots \cap M_h$ but not in M_1. The element $a+p_1 \cdots p_k$ is in none of the maximal ideals, and so must be a unit α. Since r is not one of the p_i, $r\alpha = r\prod p_i + ra$ is not divisible by any p_i, hence neither is ra, hence neither is $c=\prod p_i + ra$. But $c \in M_1$, and so must be divisible by some prime, necessarily in M_j with $j \neq 1$. This implies $\prod p_i \in M_j$, $j \neq 1$, which is impossible.

Remark. Theorem 1 may fail in rings with an infinite number of primes. For example, in the ring of integers with $(-5)^{1/2}$ adjoined, the maximal ideals $(3, 4+(-5)^{1/2})$ and $(3, 4-(-5)^{1/2})$ share the prime 3.

[1] At this juncture and at several later points, we are using the fact that any proper ideal is contained in a maximal (and hence prime) ideal. This is generally (that is, in the absence of a finiteness condition) proved with the aid of the axiom of choice, but in the present context all necessary cases are covered by the following: *a proper ideal A which is maximal in the set of all those generated by prime elements is a maximal ideal.* To prove this, we note that if A is not maximal, then there is an element c not in A such that $(c, A) \neq R$. If $c=p_1 \cdots p_m$, p_i prime, then $p_m \notin A$, hence $(A, p_m)=R$, so that $(A, p_1 \cdots p_{m-1}) \neq R$. Successively reducing m in this way, we arrive at a contradiction. Since it is evident that every prime ideal in R has a basis of primes, it follows that every prime ideal is contained in a maximal ideal. From the above statement it follows that every prime element—hence every non-unit—is contained in a maximal ideal.

We next show that any non-uniqueness of factorization already takes place within the individual maximal ideals.

THEOREM 2. *Let $M_1, \cdots, M_h$ be the maximal ideals of R, and suppose a_i, b_i are products of primes belonging to M_i, such that $a_1 \cdots a_h = b_1 \cdots b_h$. Then a_i and b_i are associates.*

Proof. The element $a_2 \cdots a_h + b_1$ is not in any of the maximal ideals, and so must be a unit α. Similarly $b_2 \cdots b_h + a_1$ is a unit β. This leads to $\alpha a_1 = \beta b_1$, as desired.

The following theorem is fundamental for the developments to follow.

THEOREM 3. *If the maximal ideal M in R has n primes $(n > 1)$, then every element of M^{n-1} is divisible by every prime of M.*

Proof. Let x be a product of $n-1$ primes of M, and suppose it is not divisible by the prime p in M. Form a sequence $x_1, \cdots, x_{n-1}$ by deleting successive factors of x: thus $x_1 = x$ and x_{n-1} is a prime. Then each $x_i + p$ is in M and so must be divisible by a prime of M, necessarily other than p or x_{n-1}. We have only $n-2$ primes with which to account for $n-1$ quantities; hence two of them, say $x_i + p$ and $x_j + p$ $(i < j)$, are divisible by the same prime q in M. Hence $x_j - x_i = x_j(1 - x_i/x_j)$ is divisible by q. But $1 - x_i/x_j$ is not in M and so is a product of primes not in M. By Theorem 2, x_j is divisible by q, which gives the absurd conclusion that p is divisible by q.

An immediate corollary is[2] the following:

THEOREM 4. *All prime ideals in R are maximal.*

Proof. Let P be a prime ideal contained in the maximal ideal M. Suppose P contains the prime p, and q is any prime in M. Then by Theorem 3, $p \mid q^{n-1}$, whence $q \in P$ and $P = M$.

To establish the chain condition in R we first prove the following theorem.

THEOREM 5. *From any sequence $\{x_i\}$ in R it is possible to select a sub-sequence $\{y_i\}$ such that $y_i \mid y_{i+1}$.*

Proof. Write $x_i = x_{i1} \cdots x_{ih}$, where $x_{ij} = 1$ or a product of primes in the maximal ideal M_j. Suppose x_{i1} is a product of n_i primes of M_1. If the n_i are bounded, some combination of primes must occur an infinite number of times. If they are unbounded, it follows from Theorem 3 that we can find a sub-sequence of $\{x_{i1}\}$ with each element dividing its successor. In either case we have a sub-sequence $\{z_i\}$ of $\{x_i\}$ whose M_1-components are successively divisible. We may now extract a further sub-sequence from $\{z_i\}$ such that each

[2] This theorem is easily proved independently of Theorems 1–3. If $P \neq M$, let $q_1, \cdots, q_m$ be the primes in M not in P, and let p be a prime in P. Then $p + q_1 \cdots q_m$ must be divisible by a prime in M, which is impossible.

M_2-component divides its successor. After h steps, we have the desired subsequence $\{y_i\}$.

It is an immediate consequence of Theorem 5 that there cannot exist an infinite sequence $\{a_i\}$ with the ideal $(a_1, \cdots, a_r)$ always properly contained in $(a_1, \cdots, a_{r+1})$. Hence we have the following theorem.

THEOREM 6. *R is Noetherian, and so is a semi-local ring in the sense of Chevalley*(3).

The following theorem shows that it is essentially possible to reduce to the case of a local ring.

THEOREM 7. *Let M be a maximal ideal in R, and R_M the quotient ring of R with respect to M. Then R_M is a local ring satisfying conditions* (a) *and* (b), *and its prime elements are just those primes of R which lie in M.*

Proof. Let $p_1, \cdots, p_n$ be the primes of R, and $p_1, \cdots, p_m$ those which lie in M. If $a/c \in R_M$, where $a, c \in R$, $c \notin M$, write $a = \alpha \prod_{i=1}^{n} p_i^{h(i)}$, where α is a unit and $h(i)$ a non-negative integer. Then

$$a/c = \left(\alpha c^{-1} \prod_{i=m+1}^{n} p_i^{h(i)} \right) \prod_{i=1}^{m} p_i^{h(i)}.$$

Since the term in parenthesis is a unit in R_M, every element of R_M is (up to a unit) a product of p_i's, $i=1, \cdots, m$. Thus no element of R_M other than $p_1, \cdots, p_m$ can be prime. Moreover the latter are prime; if, for example, p_1 is not prime, we have $p_1 = bd^{-1} \prod_{i=2}^{m} p_i^{k(i)}$, where b and d are in R but not in M. Multiplying by d, we obtain a contradiction of Theorem 2.

In conjunction with Theorem 2, Theorem 7 reduces the study of the multiplicative structure to the case of a local ring. Specifically, the multiplicative semigroup (modulo units) of R is the direct product of the corresponding multiplicative semigroups of the R_M's. There remains however a question which the authors have not investigated: can arbitrary local rings (each with a finite number of primes) be combined into a semi-local ring?

3. **Properties of local rings.** Throughout the remainder of the paper R will denote a local ring without zero-divisors which contains just n $(\geqq 3)$ prime elements. As observed in §2, the fact that R is Noetherian implies that every element of R factors into prime elements. Thus R satisfies conditions (a) and (b) of §2.

We shall denote by M the unique maximal ideal consisting of all non-units, and by K the residue class field $R-M$. The difference group $M-M^2$ may be regarded as an R-module which is annihilated by M; hence $M-M^2$ may be

[3] Cf. [1]. The definitions and fundamental results on local rings which we shall use in this paper can be found in [2] or [3]. Numbers in brackets refer to the bibliography at the end of the paper.

taken to be a vector space over K. It is easy to show [2, pp. 56–57] that a set of elements $a_1, \cdots, a_k$ will generate M if and only if the corresponding elements in $M-M^2$ generate this space over K, and that these latter elements are linearly independent over K if and only if no proper subset of $\{a_1, \cdots, a_k\}$ generates M. Thus if k is the dimension of $M-M^2$ over K, then k is also the number of elements in any minimal set of generators of M. We must have $k>1$, since if $k=1$ then $n=1$.

The nonzero elements of $M-M^2$ arise from elements of M not in M^2, and such elements must be prime and hence of the form αp_i, where α is a unit, and $p_1, \cdots, p_n$ are the primes of R. Every one-dimensional subspace of $M-M^2$ thus arises from some p_i not in M^2, so that the number of such subspaces is at most n. It follows that K is finite; the number of its elements will always be denoted by N.

If an element of R is divisible by each of $p_1, \cdots, p_n$, we shall say that it is universally divisible, or briefly that it is *universal*; a set of elements will be said to be universal if all its elements are. In this terminology, Theorem 3 asserts that M^{n-1} is universal. (This result will incidentally be considerably sharpened in the paper to follow.)

THEOREM 8. *If k is the dimension of $M-M^2$, then*

$$(N^k-1)/(N-1) \leqq n, \tag{1}$$

with equality holding if and only if M^2 is universal. If there is a prime in M^2, then

$$(N^{k+1}-1)/(N-1) \leqq n. \tag{2}$$

Proof. Since $M-M^2$ is of dimension k over a field of N elements, it has N^k-1 nonzero elements, hence $(N^k-1)/(N-1)$ one-dimensional subspaces; (1) then follows from a remark above. If M^2 is not universal, then there exist primes p_h, p_i, p_j such that p_hp_i is not divisible by p_j. Hence if $p_hp_i+p_j$ is divisible by p_l, then $l\neq j$, p_j and p_l cannot give rise to distinct one-dimensional subspaces, and so strict inequality holds in (1). Conversely, if strict inequality holds, then there exist primes p_j and p_l $(j\neq l)$ such that $ap_j+bp_l\in M^2$, where a and b are in R, but not both in M. If, say, a is a unit, then ap_j+bp_l cannot be divisible by p_l, and M^2 is not universal.

Suppose there is a prime q in M^2. Let $p_1, \cdots, p_m$ be a set of primes giving rise to the $m=(N^k-1)/(N-1)$ one-dimensional subspaces of $M-M^2$, and let $u_1, \cdots, u_N$ be a set of representatives in R of the elements of K. None of the Nm elements p_i+u_jq $(1\leqq i\leqq m,\ 1\leqq j\leqq N)$ is in M^2, hence they are all prime. If any two were associates, we would have $p_h+u_lq=\alpha(p_i+u_jq)$, α a unit. Since $p_h-\alpha p_i\in M^2$, we must have $h=i$ and $\alpha\equiv 1 \pmod{M}$. It follows that $(u_l-\alpha u_j)q$ is divisible by p_i, so that $u_l-\alpha u_j$ and hence also u_l-u_j is a non-unit, whence $l=j$. Thus we have Nm non-associated primes not in M^2, so that

$$N(N^k - 1)/(N - 1) + 1 \leqq n,$$

and (2) follows.

It is to be noted that we always have $N \leqq n-1$, and that the extreme case $N=n-1$ entails that $k=2$ and M^2 is universal.

Whether or not there exist rings with a prime in M^2 is a question that has not yet been settled. It follows from (2), and the fact that k and N are at least 2, that such a ring must have at least seven primes. Since we shall prove below that M^2 is universal when n is prime, the lower bound becomes $n=8$. We shall continue this discussion in the second paper; but we remark that at the moment our best result has ruled out the possibility of a prime in M^2 for $n=8$ or 9.

Since R is a local ring, it is known [2, p. 59] to admit a unique "completion." The following theorem shows that, for multiplicative purposes, we may without loss of generality pass to this completion.

THEOREM 9. *The completion R^* of R has no zero-divisors and has exactly the same primes as R does.*

Proof. Let M^* be the maximal ideal of R^*, so that $M^* = R^* \cdot M$. By Theorem 3, $M^n \subseteq R \cdot p_i$, hence $M^{*n} \subseteq R^* \cdot p_i$ for $i=1, \cdots, n$. We show that every a^* in R^* is the product of a unit in R^* and of p's. This will be shown by induction on h, where $a^* \in M^{*h}$, $a^* \notin M^{*h+1}$. The case $h=0$ is trivial, so we assume $h \geqq 1$. Since $a^* \in M^*$, there is an $a \in M$ such that $a^* \equiv a \pmod{M^{*n}}$. Now a is divisible by some p_i, $a \in R \cdot p_i$, hence $a^* \in (R^* \cdot a, M^{*n}) \subseteq R^* \cdot p_i$. Thus $a^* = b^* p_i$, and since $b^* \notin M^{*h}$, the induction assumption applied to it gives the factorization for a^*.

This factorization shows that R^* has no zero-divisors and that its primes lie among $p_1, \cdots, p_n$. Moreover these latter are prime; if p_1 were not prime, we would have $p_1 \in R^* \cdot p_i p_j \cap R = R \cdot p_i p_j$, which is absurd.

For later use we insert at this point the following theorem.

THEOREM 10. *There exist N primes $q_1, \cdots, q_N$ such that $q_i | xq_j$ for every i, j and for every $x \in M$.*

Proof. Let h be the integer for which M^h is not universal but M^{h+1} is, and suppose $y \in M^h$ is not divisible by the prime q. Let $u_1, \cdots, u_{N-1}$ be representatives in R of the nonzero elements of the residue class field K. Let r_i be a prime divisor of $y + u_i q$. It is impossible that r_i and r_j $(i \neq j)$ be the same, for then $r_i | (u_i - u_j)q$; since $u_i - u_j$ is a unit, r_i and q would be associates, a contradiction. Multiplying $y + u_i q = r_i \cdots$ by a non-unit x, we find that $r_i | xq$. Thus we have $N-1$ distinct primes which divide xq for any $x \in M$. Let us denote any of these primes by an $(N-1)$-valued function $f(q)$.

It is clear that each r_i, like q, is a non-divisor of y. Hence the f operator may be applied to them in turn, and in general f may be indefinitely iterated. We now assert that it is possible to find k distinct primes $q_1, \cdots, q_k$ $(k \geqq N)$

with $q_{i+1}=f(q_i)$ $(i=1, \cdots, k-1)$ and $q_1=f(q_k)$. For the denial of this assertion permits us to construct an infinite chain $\{s_i\}$ of distinct primes, with $s_i=f(s_{i-1})$, as follows. Take $s_1=q$, and suppose s_i chosen for $i<m$. Of the $N-1$ primes given by $f(s_{m-1})$, we can choose one distinct from the $N-2$ primes $s_{m-N+1}, \cdots, s_{m-2}$; this is our choice for s_m. Moreover s_m must be distinct from s_j for $j\leqq m-N$, for otherwise $s_{j+1}, \cdots, s_m$ would be the desired set of q's. Thus the process of selecting primes s_m can be continued indefinitely, contradicting the finiteness of the number of primes.

Now any multiple of q by a non-unit is a multiple of $f(q)$ by a non-unit; hence the cyclic closure under f of the set $q_1, \cdots, q_k$ leads to $q_i | xq_j$ for any i, j, and any $x\in M$. The first N of the q's provide a set of the kind required in the theorem.

4. **A decomposition of semigroups.** Let S be a commutative semigroup, that is, a system with a commutative and associative multiplication such that $xy=xz$ implies $y=z$. It is known that S can be embedded in a certain smallest group G, called the quotient group. Assume further that S has a unity element 1, but no other units—that is, $xy=1$ implies $x=y=1$. Let M be the set S with 1 omitted and V the set of elements a of G with $aM\subseteq M$, $a^{-1}M\subseteq M$; clearly V is a subgroup of G. If p is a prime of S (an element whose only factorization in S is $p\cdot 1$), and v is any element in V, then pv is a prime; for a factorization $pv=xy$ would lead to $p=x(yv^{-1})$. Thus a coset mod V of a prime consists exclusively of primes.

Suppose now that S contains exactly n primes $p_1, \cdots, p_n$, and that any element of S can be factored into a product of p's. Then it follows from the above that s, the order of V, must be a divisor of n. The primes split into $t=n/s$ cosets of s each, say as p_{ij} $(i=1, \cdots, t; j=1, \cdots, s)$. For any fixed i, the set $\{p_{ij}/p_{i1}\}$ is precisely the group V. In particular, if $s=n$, the elements $\{p_j/p_1\}$ constitute V, and S is completely determined as the direct product of V and the infinite cyclic semigroup generated by p_1. It is to be observed that $s=n$ characterizes the case where M^2 is universal, that is, where the product of any two primes is divisible by any third prime.

Let us now apply these results to the case where S is the multiplicative semigroup of R, reduced modulo units. Let $q_1, \cdots, q_N$ be a set of primes whose existence is guaranteed in Theorem 10. Then each q_i/q_1 is readily seen to be a member of V, and we have that s, the order of V, is at least N. In summary we may state the following theorem.

THEOREM 11. *The n primes split into t sets of s each $(s\geqq N)$: p_{ij} $(i=1, \cdots, t;$ $j=1, \cdots, s)$, such that for any fixed i the set $\{p_{ij}/p_{i1}\}$ forms a multiplicative group modulo units. The case M^2 universal is characterized by $s=n$, $t=1$, and in that case the set $\{p_j/p_1\}$ $(j=1, \cdots, n)$ forms a multiplicative group modulo units.*

In the special case where n is prime, $s|n$ and $s\geqq N\geqq 2$ imply that $s=n$. Hence we have:

COROLLARY. *When n is prime, M^2 is universal.*

5. **The case of M^2 universal.** Let R be a local ring with primes $p_1, \cdots, p_n$ in which M^2 is universal. The latter condition implies that if $y \in M^2$, then any p_i divides y, and in fact $y/p_i \in M$. Let T be the set of all a/p where $a \in M$ and p is a fixed prime; T is clearly a ring containing R, and M is a proper ideal in T. Hence if a/p is a unit in T, then $a/p \notin M$, $a \notin M^2$ and $a = \alpha p_i$, α a unit in R. Conversely, every element $\alpha p_i/p$ is a unit in T, since by Theorem 11 the p_i/p form a multiplicative group modulo units (of R). It follows that M consists precisely of all non-units of T. Every proper ideal of T, being thereby contained in M, is an ideal in R and hence is finitely generated. Thus T is a local ring, and since $M = p \cdot T$ is principal, it is a discrete valuation ring. In fact T is the integral closure of R, for clearly $T = R[p_1/p, \cdots, p_n/p]$, and p_i/p is integrally dependent on R since, by Theorem 11, $(p_i/p)^n$ is a unit in R.

Let L be the residue class field $T-M$. Since residue classes of R pass in their entirety into residue classes of T, we may suppose that L contains $K = R-M$. Let R_0, T_0, K_0, L_0 be the multiplicative groups of units of R, T, K, L respectively. The group T_0 has a natural homomorphism on L_0, which in turn is homomorphic to L_0/K_0. The resulting homomorphism of T_0 on L_0/K_0 has R_0 as its kernel. For T_0 consists of elements $\alpha p_i/p$ $(\alpha \in R_0)$; if such an element maps on the identity of L_0/K_0, then its map in L_0 is in K_0. Hence there is a unit β in R_0 such that $\alpha p_i/p - \beta \in M$, $\alpha p_i - \beta p \in M^2$. Since p divides every element of M^2, it must divide p_i, so that $p = p_i$ and $\alpha p_i/p \in R_0$. Thus $T_0/R_0 \cong L_0/K_0$. Since T_0/R_0 is isomorphic to the group of p_i/p_1, mod units, the order of L_0/K_0 is n, which equals $(N^k-1)/(N-1)$ by Theorem 8. Since K_0 contains $N-1$ elements, L_0 contains N^k-1, and $[L:K]=k$. Moreover L_0/K_0, and hence T_0/R_0, is cyclic. Collecting these facts we have:

THEOREM 12. *Let R be a local ring with primes $p_1, \cdots, p_n$ and a residue class field of N elements, and suppose M^2 is universal. Then the multiplicative structure of R is determined by the fact that the set $\{p_i/p_1\}$ forms a cyclic group under multiplication, modulo units. If R is complete and not of characteristic zero, then R is uniquely determined.*

It remains to prove the final statement. Let R_1 be another complete local ring with the same n and N and with M_1^2 universal. We observe that the valuation ring T is complete [2, p. 68] and has the same characteristic as its residue class field, which contains N^k elements. The same can be said of the valuation ring T_1 determined by R_1, k being the same in both cases since it is determined by n and N. The residue class fields are thus isomorphic and hence so are T and T_1 [5]. This isomorphism between T and T_1 will carry R into R_1 since we can characterize R within T in an invariant way. Namely, we assert that R consists of all elements $x \in T$ such that $x^N \equiv x$ (mod M). For this is clearly satisfied if $x \in R$. Conversely suppose the congruence holds. Then the residue of x is in K, hence $x \equiv \alpha$ (mod M) where $\alpha \in R$, and $x \in R$.

The uniqueness asserted in Theorem 12 fails if R is allowed to have characteristic zero. For it is well known that the corresponding T is not uniquely determined if it has characteristic zero. Indeed it is easy to construct an infinite number of non-isomorphic rings R in this characteristic unequal case.

A sort of converse of Theorem 12 holds, and it assures us of the existence of a class of nontrivial rings with n primes.

THEOREM 13. *If N is a power of a prime integer, and $n=(N^k-1)/(N-1)$, $k\geqq 2$, then there exists a local ring with n primes, with a residue class field of N elements, and with M^2 universal.*

Proof. The construction is suggested by the above characterization of R within T. Let L be a field of N^k elements and let [4, Theorem 2] T be a discrete valuation ring with L as residue class field. Now L contains a (unique) subfield K of N elements. Let R consist of all elements of T whose residues are in K; R is clearly a ring. The set M of all elements of R with residue 0 is an ideal, and all non-units of T are in M. Also all non-units of R are in M. For if $a\in R$, $a\notin M$, then a is a unit in T, and the residue of σ^{-1} is in K; hence $a^{-1}\in R$, and a is a unit in R. Thus M is the ideal of non-units in R.

Let p be the prime element of T. The multiplicative group L_0 of nonzero elements of L has $(N^k-1)/(N-1)=n$ cosets mod K_0; from each we pick one element, and then we select representatives $\theta_1, \cdots, \theta_n$ of these in T. Let $p_i=\theta_i p$. Clearly each $p_i\in M$, and we show next that each $a\in M$ is a product of p_i's. Now $a=\alpha p^m$, α a unit in T, $m\geqq 1$. Hence also $a=\theta p p_1^{m-1}$, θ a unit in T. It is then sufficient to show that $\theta p/p_i$ is a unit in R for some i. But $\theta p/p_i=\theta/\theta_i$, and from the definition of the θ_i's, it follows that for some i, θ/θ_i has residue in K. Thus the primes of R lie among the p's. That they are all primes, and non-associated—that is, that no p_i/p_j can be in R—follows from the fact that no θ_i/θ_j can have residue in K. Thus R has just n primes. For any h, i, j, $p_h p_i/p_j\in R$, so that M^2 is universal.

As a result of this theorem, it is seen that it is a purely number-theoretic question to determine what values of n and N admit rings with M^2 universal. It should be noted that n does not uniquely determine N, for example, $31=(5^3-1)/(5-1)=(2^5-1)/(2-1)$.

In particular, the study of rings with a prime number of primes is now entirely number-theoretic. The smallest prime with no corresponding ring is 11. The following table shows the possible values of n less than 1000, and the corresponding N:

n	3	5	7	13	17	31	31	73	127	257	307	757
N	2	4	2	3	16	2	5	8	2	256	17	27.

Both the Mersenne numbers 2^k-1, and the Fermat numbers $2^{2^m}+1$ play a role in this connection: the former for $N=2$, the latter for $k=2$, $N=2^{2^m}$.

Thus the question of whether there exist an infinite number of rings with a prime number of primes is intimately connected with famous unsolved problems of number theory.

Bibliography

1. C. Chevalley, *On the theory of local rings*, Ann. of Math. vol. 44 (1943) pp. 690-708.

2. I. S. Cohen, *On the structure and ideal theory of complete local rings*. Trans. Amer. Math. Soc. vol. 59 (1946) pp. 54-106.

3. W. Krull, *Dimensionstheorie in Stellenringen*, J. Reine Angew. Math. vol. 179 (1938) pp. 204-226.

4. S. MacLane, *Subfields and automorphism groups of p-adic fields*, Ann. of Math. vol. 40 (1939) pp. 423-442.

5. E. Witt, *Zyklische Körper und Algebren der Charakteristik p vom Grad p^n*, J. Reine Angew. Math. vol. 176 (1937) pp. 126-140.

Harvard University,
Cambridge, Mass.
University of Chicago,
Chicago, Ill.